UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/740,748	12/19/2003	Tin Qian	224180	4932

45840 7590 04/16/2007

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
WANG, HARRIS C	
ART UNIT	**PAPER NUMBER**
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/740,748	QIAN ET AL.	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/25/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.

Claims 1-6 have been canceled

Claims 7-10, 12-13, 19, 21-24 are amended

Claims 11, 14-18, 25-31 are original.

Claim Rejections - 35 USC § 112

2.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 7-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claims 7, 19 and 24 Applicant has amended claims to include the "policies specified in said user-centric form." User-centric form for policies is not a well known term in the art. In the Paragraph [0054] of the specification Applicant writes that "The setting editor class object provides firewall and policy management software developers a programmatic interface to manage firewall policy in a simple and application and user-centric form." Although it is clear that the policy is centered around the user in some way, no examples or definitions further limit the scope of what user-centric specifically means.

Claims 8-13, 20-23 and 25-31 are dependent on the independent claims 7, 19 and 24 and are rejected for the same rationale.

Response to Arguments

3.

Applicant has amended the Claims to include both a "first user", which specifies policies in packet-centric form, and a "second user", which specifies policies in user-centric form. Although the Applicant never explicitly mentions a first or second user the Applicant does describe:

"The policy object model is used to specify policies that the services support. The policy object model permits an advanced user to define traditional packet-centric type filtering policy, or a less advanced user to develop policy using more simplified rules" (Paragraph [0010]).

Therefore the Examiner interprets that both the first user and second user are administrators, where the first user assigns policies based on traditional firewall rules and the second user assigns policies based on application level rules.

Applicant argues that regarding the Object Model of Claim 7, the Method of Claim 19 and the Object Model of Claim 19, Terzis neither discloses or suggest "a policy object model for specifying, by a first user, one or more policies that the service supports in a packet-centric form." Terzis in Paragraph [0089] teaches *"the subsystems include a firewall...The firewall operates at layer 4 (transport)...The firewall serves to prevent*

unauthorized access of a network...by filtering out packets that originate from unauthorized users or sources. Performing filtering of packets can be effective in deterring certain types of unauthorized access attempts, but requires inspection of each packet."

and by a second user, said one or more policies in a user-centric form and/or an application-centric form" *("The policies can be determined both by the identity of the user as well as by the group the user is associated with...Based on the policies associated with that user, a set of specific access rules are generated that enable the subsystems to provide filtering and deny access to prohibited resources and services" Paragraph [0089])*

Figure 14 shows the policy engine (1420) communicating with both the L3 & L4 Rules DB (1435) as well as the L7 Rules DB (1430). The Examiner interprets the L3 & L4 Rules as packet-centric policy rules and the L7 rules as the user-centric policy rules.

Figure 6 shows the policy objects. *Terzis (Paragraph 0118) teaches "The policy rules are an abstract class that all policy rules derive from...The resource access rules are used to control which users have access to what resources (Paragraph 0120)...The security rules 690 may describe how packets matching the source, destination objects should be secured (Paragraph 0130).* The Examiner interprets the policies based on the resource access rules as user-centric and the policies based on the security rules as packet-centric.

Applicant further argues that Terzis does not disclose nor suggest; "a policy engine platform for interacting of said user with said one or more policies specified in said packet-centric form and of said second user with said one or more policies specified in said user-centric form and/or said application-centric form," *("The policy interpreter interfaces to the SNMP Agent" Paragraph [0064], Fig. 7)*

The Examiner interprets the policy object model as the "policy engine" and policy engine platform as "policy interpreter." As described above policies can be both packet-centric and user-centric.

As seen in Fig. 7, the Policy Interpreter acts as a intermediary between the SNMP agent and the Policy engine. Because the purpose of a SNMP agent is to facilitate information between network components and the purpose of the policy engine is to provide policies, it is inherent that the policy interpreter will provide one or more policies of which one will actually perform the service.

Applicant's arguments with respect to claims 7-31 are have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 7-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Terzis (US 20040243835).

Regarding Claim 7,

Terzis teaches an object model for managing a service on a computer, the object model comprising:

a policy object model for specifying, by a first user, one or more policies that the service supports in a packet-centric form *("the subsystems include a firewall...The firewall operates at layer 4 (transport)...The firewall serves to prevent unauthorized access of a network...by filtering out packets that originate from unauthorized users or sources. Performing filtering of packets can be effective in deterring certain types of unauthorized access attempts, but requires inspection of each packet" Paragraph [0089])*, and, by a second user, said one or more policies in a user-centric form and/or application-centric form; *("the policy engine talks to the components on the data plane to install and remove filters in response to policy rules," Paragraph [0062]) ("The policies can be determined both by the identity of the user as well as by the group the user is associated with...Based on the policies associated with that user, a set of specific access rules are generated that enable the subsystems to provide filtering and deny access to prohibited resources and services" Paragraph [0089])*

and a policy engine platform for interacting of said first user with said one or more policies specified in said packet-centric form and of said second user with said one or more policies specified in said user-centric form and/or said application-centric

form and to provide said one or more policies to said at least one component that actually performs the service. *("The policy interpreter interfaces to the SNMP Agent," Paragraph [0064], Fig 7.)*

The Examiner interprets the policy object model as the "policy engine" and policy engine platform as "policy interpreter."

As seen in Fig. 7, the Policy Interpreter acts as a intermediary between the SNMP agent and the Policy engine. Because the purpose of a SNMP agent is to facilitate information between network components and the purpose of the policy engine is to provide policies, it is inherent that the policy interpreter will provide one or more policies of which one will actually perform the service.

Regarding Claims 8 -10,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a rule editor for adding an additional policy by said first user in accordance with the policy object model, wherein the rule editor is also configured to delete a policy by said first user, wherein the rule editor is also configured by said first user to edit a policy.

("The interface between the policy engine and the SNMP agent may be used to add and delete policy objects" Paragraph [0064])

The Examiner interprets that editing a policy is the same as adding or deleting a policy. The Examiner interprets the first user to be an administrator that implements

packet-centric policies. (*The security rules 690 may describe how packets matching the source, destination objects should be secured. Paragraph [0130]*)

Regarding Claims 11 and 12,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a setting editor configured to automatically generate a policy based upon an application and user combination, wherein the setting editor generates a plurality of policies, and is further configured to permit said second user to select from the plurality of policies.

("After a user has successfully logged [in]...the Launch-pad module may contact the policy engine to receive the list of resources that are available to that user...Once fount the policy user may return each of the resources in those rules back to the Launch-pad module, Paragraph [0065])

Where the Launch-pad is defined as a user interface in Paragraph 100. The launch pad screen is capable of displaying "applications...that are specifically made available to that user (Paragraph 106).

The Examiner interprets the second user to be an administrator that implements user-centric policies. *(The resource access rules are used to control which users have access to what resources. Paragraph [0120]*)

Regarding Claim 13,

Terzis teaches the object model of claim 12, wherein the setting editor is further configured by said second user to permit setting one of the plurality of policies as a default policy.

("generating, based on the access policies, at least one access rule for each of a plurality of security system sublayers," Claim 1).

The Examiner interprets the at least one access rule as the default policy.

The Examiner interprets the second user to be an administrator that implements user-centric policies. *(The resource access rules are used to control which users have access to what resources. Paragraph [0120])*

Regarding Claim 14,

Terzis teaches the object model of claim 7, wherein the policy engine platform comprises a rule explorer for providing a view of the one or more policies.

Because the policy interpreter interfaces between the SNMP agent and the policy engine (Fig. 7) it is inherent that there will be a component that allows a view of one or more of the policies.

Regarding Claim 15,

Terzis teaches the object model of claim 7, wherein the policy object model comprises a policyrule object usable to generate policy, the policyrule object

comprising a condition property and an action property, wherein a policy generated by the policyrule object is configured to perform an action in the action property responsive to a condition in the condition property being met. (Fig. 6, 670)

Regarding Claim 16,

Terzis teaches the object model of claim 7, wherein the service is a firewall service. *("According to one embodiment the rules are generated and installed at the firewall level" Paragraph [0019])*

Regarding Claim 17,

Terzis teaches the object model of claim 7, wherein the policy engine platform is configured to deny providing said one or more policies to the component if a requester is not authorized. ("*Based on the policies associated with that user, a set of specific access rules are generated that enable the subsystems to provide filtering and deny access to prohibited resources and services." Paragraph [0088])*

Regarding Claim 18,

Terzis teaches the object model of claim 17, wherein determining whether a requester is authorized comprises comparing a provider rank for the requester against

a permitted rank, and if the provider rank for the requestor does not meet or exceed the permitted rank, denying the requester. (Fig 6. 675, PermissionLevel)

The Examiner interprets the parameter PermissionLevel under the Resource Access Rules as rank. Where the PermissionLevel is checked against a permitted PermissionLevel and if the PermissionLevel does not meet or exceed the permitted rank, to deny the requestor.

Regarding Claim 19,

Terzis teaches a method of managing a service on a computer, the method comprising: specifying, via a policy object model, by a first user, one or more policies that the service supports in a packet-centric form, and, by a second user, said one or more policies in a user-centric form and/or an application-centric form; *("The policy engine talks to the components on the data plane to install and remove filters in response to policy rules," Paragraph [0062])*

and interacting, via a policy engine platform, of said first user with said one or more policies specified in said packet-centric form, and of said second user with said one or more policies specified in said user-centric form and/or said application-centric form; *("the Launch-pad module may contact the policy engine to receive the list of resources that are available" Paragraph [0065])*

and providing, via the policy engine platform, said one or more policies to said at least one component that actually performs the service. *("Once found the policy engine*

may return each of the resources in those rules back to the Launch-pad module" Paragraph [0065])

Terzis teaches "the subsystems include a firewall...The firewall operates at layer 4 (transport)...The firewall serves to prevent unauthorized access of a network...by filtering out packets that originate from unauthorized users or sources. Performing filtering of packets can be effective in deterring certain types of unauthorized access attempts, but requires inspection of each packet. (Paragraph [0089])." Terzis further teaches ""The policies can be determined both by the identity of the user as well as by the group the user is associated with...Based on the policies associated with that user, a set of specific access rules are generated that enable the subsystems to provide filtering and deny access to prohibited resources and services" Paragraph [0089])

The Examiner interprets the first user to be an administrator that implements packet-centric policies. (*The security rules 690 may describe how packets matching the source, destination objects should be secured. Paragraph [0130])*

The Examiner interprets the second user to be an administrator that implements user-centric policies. *(The resource access rules are used to control which users have access to what resources. Paragraph [0120])*

Regarding Claim 20,

Terzis teaches the method of claim 19, further comprising automatically generating a policy based upon an application and user combination. *"After a user has successfully logged into the MACSS, the Launch-pad module may contact the policy engine to receive the list of resources that are available to that user," Paragraph [0065])*

Regarding Claim 21,

Terzis teaches the method of claim 20, further comprising generates a plurality of policies, and permitting a user to select from the plurality of policies. *("Once found the policy engine may return each of the resources in those rules back to the Launch-pad module" Paragraph [0065])*

As described before the Launch-pad module is a user interface. Examples can be found in Fig. 4 and Fig. 5.

Regarding Claim 22,

Terzis teaches the method of claim 21, further comprising setting one of the plurality of policies as a default policy. *("generating, based on the access policies, at least one access rule for each of a plurality of security system sublayers," Claim 1)*

The Examiner interprets the at least one access rule as the default policy.

Regarding Claim 23,

Terzis teaches the method of claim 22, further comprising authorizing a user prior to providing said one or more policies. *("the Launch-pad module may contact the policy engine to receive the list of resources that are available" Paragraph [0065])*

Regarding Claim 24,

An object model embodied on a computer-readable medium for managing a firewall service on a computer, the object model comprising a policy object model used to specify, by a first user, one or more policies that the firewall service supports in a packet-centric form, and, by a second user, said one or more policies in a user-centric form and/or application-centric form, the policy model comprising a policyrule object usable to generate policy *(Fig. 6, PolicyRule, 670)*, the policyrule object comprising a condition property and an action property, wherein a policy generated by the policyrule object is configured to perform an action in the action property responsive to a condition in the condition property being met.

It is inherent that the policy rule is configured to perform an action responsive to a condition being met.

Terzis teaches "the subsystems include a firewall...The firewall operates at layer 4 (transport)...The firewall serves to prevent unauthorized access of a network...by filtering out packets that originate from unauthorized users or sources. Performing filtering of packets can be effective in deterring certain types of unauthorized access attempts, but requires inspection of each packet. (Paragraph [0089])." Terzis further teaches ""The policies can be determined both by the identity of the user as well as by the group the user is associated with...Based on the policies associated with that user, a set of specific access rules are generated that enable

the subsystems to provide filtering and deny access to prohibited resources and services" Paragraph [0089])

The Examiner interprets the first user to be an administrator that implements packet-centric policies. (*The security rules 690 may describe how packets matching the source, destination objects should be secured. Paragraph [0130])*

The Examiner interprets the second user to be an administrator that implements user-centric policies. *(The resource access rules are used to control which users have access to what resources. Paragraph [0120])*

Regarding Claim 25,

Terzis teaches the object model of claim 24, further comprising an IPSecRule derived from the policyrule object, the IPSecRule being configured to trigger an IPSec callout when an IPSec condition is matched, and to indicate configuration parameters for securing traffic related to the callout. (Fig. 14, 1440).

The services dispatcher connects to the launch-pad which connects to the policy engine.

Regarding Claim 26,

Terzis teaches the object model of claim 25, wherein the IPSecRule evaluates a standard 5-tuple to determine if a condition has been met. (Fig. 11)

Regarding Claim 27,

The object model of claim 24, further comprising a KeyingModuleRule derived from the policyrule object, the KeyingModuleRule being configured to select which key negotiation module to use when there is no existing secure channel to a remote peer.

("The key exchange field specifies how keys are exchanged and determines what key parameters will be used." Paragraph [0130])

The Examiner interprets key negotiation as key exchange. The Examiner notes that the key exchange field is part of the security rules, which is part of the policy rules.

Regarding Claim 28,

Terzis teaches the object model of claim 27, wherein the KeyingModuleRule evaluates a standard 5-tuple to determine if a condition has been met. (Fig. 11)

Regarding Claim 29,

Terzis teaches the object model of claim 24, further comprising a IKERule derived from the policyrule object and configured to specify the parameters for carrying out Internet Key Exchange key negotiation protocol. (Fig. 14, IKE)

Regarding Claim 30,

Terzis teaches the object model of claim 29, wherein the IKERule evaluates a local address and a remote address to determine if a condition has been met. This step is inherent in IKE protocol.

Regarding Claim 31,

Terzis teaches the object model of claim 29, wherein the IKERule comprises an IKEAction action property that defines the authentication methods for performing Internet Key Exchange key negotiation protocol. *("The key exchange field specifies how keys are exchanged and determines what key parameters will be used." Paragraph [0130])*

Conclusion

5.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Taghi T. Arani
Primary Examiner
T. Arani
4/11/04